PRIVACY IMPACT ASSESSMENT (PIA)

For the

improved Investigative Records Repository
Defense Manpower Data Center

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 9878
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI 2880

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 13 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ **Yes**

Enter OMB Control Number | In Progress

Enter Expiration Date |

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 615, Armed Forces, Information furnished to selection boards; E.O. 10450, Security Requirements for Government Employment; DoD Directive 5200.2, Department of Defense Personnel Security Program; DoD Directive 5200.27 (Section IV A and B), Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense; DoD Instruction 5210.91, Polygraph & Credibility Assessment Procedures; DoD Directive 5220.6, Defense Industrial Personnel Security Clearance Program Review; DoD Directive 5220.28, Application of Special Eligibility and Clearance Requirements in the SIOP-ESI Program for Contractor Employees, and 18 U.S.C. 3056, Powers and Duties of the Secret Service and E.O. 9397, as amended (SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

To ensure that the acceptance or retention of persons in sensitive DoD positions or granting individuals including those employed in defense industry access to classified information is clearly consistent with national security. To determine the loyalty, suitability, eligibility, and general trustworthiness of individuals for access to defense information and facilities. To determine the eligibility and suitability of individuals for entry into and retention in the Armed Forces. To provide information pertinent to the protection of persons under the provisions of 18 U.S.C. 3056, Powers and Duties of the Secret Service. For use in criminal law enforcement investigations, including statutory violations and counterintelligence as well as counterespionage and other security matters. For use in military boards selecting military members for promotion to grades above 0-6.
PII to include: Name, SSN, Date of Birth, Gender. Information related to investigation reports, case control and management documents.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Improper management, handling, transmission or use of IIRR files by DMDC employees or accredited IIRR data requesters may cause serious harm to an IIRR file subject's personal life, professional career, and/or impact National Security interests.

- The facility where the IIRR system and IIRR operations take place is a high security underground repository.
- The IIRR database is a standalone system that cannot be accessed by anyone but vetted DMDC employees.
- IIRR files are only distributed to accredited requesters that work for accredited agencies or Federal FOIA/PA offices.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. OSD, WHS, DSS, DIA, DLA, DISA, DOHA, DVA, DODIG, USDI

☒ **Other DoD Components.**

Specify. Army, Navy, Marine Corps, Air Force

☒ **Other Federal Agencies.**

Specify. OPM, DOJ, DOS, DOL, HUD, FBI, DHS, USDA, NASA, IRS, FAA

☒ **State and Local Agencies.**

Specify. State and Local Law Enforcement

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Contractor Names TBD based on current contract - standard PII protection verbiage.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Information provided by individuals for a security clearance is voluntary. Without voluntary disclosure of information on an SF86 an investigation cannot be completed in a timely manner and may negatively affect an individuals placement or security clearance prospects.

If an individual objects to sharing the required personal information needed to initiate a security clearance then the individuals clearance request cannot be processed.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Information in an IIRR investigation may be disclosed without the individuals consent as permitted by the Privacy Act (5 USC 552a (b).

IIRR files are completed security clearances for individual subjects based upon the individuals Standard Form 86 Electronic Personnel Security Questionnaire (SF86 EPSQ). The SF86 EPSQ is used to initiate or reinvestigate a persons eligibility for security clearance access. The SF86 EPSQ provides a list of Privacy Act Routine Uses under which a subjects IIRR file information may be accessed by other than the person who is the subject of the SF86 EPSQ. When a subject signs and submits their SF86 EPSQ they consent to those Privacy Act Routine Uses.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐	**Privacy Act Statement**	☒	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.	Collection, maintenance, and disclosure of background investigative information is governed by the Privacy Act. These Privacy Act applications are acknowledged by the individuals signature on their SF86 EPSQ and in interviews between the individual and their clearance investigator. Information in an IIRR investigation may be disclosed without the individuals consent as permitted by the Privacy Act (5 USC 552a (b). IIRR files are completed security clearances for individual subjects based upon the individuals Standard Form 86 Electronic Personnel Security Questionnaire (SF86 EPSQ). The SF86 EPSQ is used to initiate or reinvestigate a persons eligibility for security clearance access. The SF86 EPSQ provides a list of Privacy Act Routine Uses under which a subjects IIRR file information may be accessed by other than the person who is the subject of the SF86 EPSQ. When a subject signs and submits their SF86 EPSQ they consent to those Privacy Act Routine Uses.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.